Practical Security Considerations For IoT Systems Over Satellite

Joan Bas*, Ana Pérez-Neira*†
*{joan.bas, marius.caus, ana.perez}@cttc.es, AMSP Department, CTTC/CERCA,Castelldefels,Spain
† Dept. of Signal Theory and Communications Universitat Politècnica de Catalunya, Barcelona, Spain

Abstract

Currently, the forecast for the European market for IoT is a yearly 19.8% increase up to reach $241 billion in 2025. This strong growing will be concentrated in verticals from manufacturing, utilities, retail and transportation [1], [2]. However, in order to monetize the potential services over IoT it is necessary to guarantee the security of the communications [3]. In this regard physical-layer security methods may complement higher-layer encryption techniques by exploiting the characteristics of wireless channels. For this purpose, it is resorted to the secrecy-capacity metric to measure the security level. More specifically, it was shown in [4] that reliable information-theoretic security could be achieved, whenever the eavesdropper's channel be a degraded version of the legitimate user's channel. In this case, if the secrecy rate is chosen below the secrecy-capacity, then reliable transmissions can be achieved in perfect secrecy. However, the time-varying fading effect of wireless channels degrades the secrecy-capacity. In this situation, it is used the ergodic capacity to measure the secrecy-capacity [5]. In order to make the overhearing process of the eavesdroppers difficult, it is used the time-packing/faster than Nyquist strategy [6]- [7].Thus, the time-duration of the transmitted frames are reduced which: i) improves the interception probability of the packets, ii) augments the spectral efficiency of the M2M communications without increasing the transmission bandwidth, iii) diminishes the effect of Doppler spread in Non-GEO communications, and iv) permits to use the overlapping degree among the pulse shapes to boost the secrecy-capacity. On the contrary, this overlapping degree introduces a multi-path channel that may difficult the synchronization process. However, the coefficients of the multipath channel are known by the legitimate user but ignored by the eavesdropper. This strategy of security is similar to that the Artificial Noise (AN) one pursues [5], [8]- [9], but without wasting energy for jamming the eavesdropper's channel.

Note that the satellite channel model has a large Line of Sight (LoS) component. So, it means that the channel of the eavesdropper and the legitimate user could be quite similar in the same beam of the satellite constellation. So it is necessary to distort the channel of the desired user in order to increase the security of the communications. The use of non-Nyquist pulses, permits to introduce an artificial multipath interference that degrades the eavesdropper's channel. In this case, we have considered two types of eavesdropper: i) without being able to estimate the time-packing multipath, and ii) equipped with an estimation block of the time-packing interference. In the first case, all interference signals are considered as noise whereas in the second one part of the interference is assumed as noise. In both cases, it is possible to obtain a secrecy-capacity. Finally, comment that in satellite constellation there is a residual co-channel interference. This interference limits the resolution of the eavesdroppers although they be equipped with multiple antennas. We have considered that the eavesdropper does not have full knowledge of the time-packed/faster than Nyquist multi-path interference. This pragmatic approach was also followed in [9]. However, there the rain losses made difficult to obtain perfect channel estimations.

I. Introduction

A. Review of the State-Of-The-Art on Physical Layer Security

In order to provide a certain level of security in a communication system it is generally resorted to cryptography. Nonetheless, it requires a non-negligible power for encryption and decryption the plaintext message [10]. Moreover, cryptographic strategies assume that the eavesdropper has a limited computational burden and rely on their difficulty on unveiling a message that has been protected by means of cryptography. However, its security may be compromised if an efficient method for solving the cryptographic keys is discovered. In addition the physical radio wireless channel can be altered either by a fading or intentional jamming. As a results, it emerges physical layer security techniques, which can be used to complement the cryptographic ones. Specially this technique can be of utility in IoT domain since the IoT devices are power limited, which condition the use of complex cryptographic schemes [11]. Physical layer security techniques were initially investigated by Wyner [4] for providing secrecy when the wiretap channel was memoryless. There it was shown that perfect secure transmissions could be achieved if the transmission rate of the legitimate transmitter falls in the outage rate region of the eavesdropper. Currently, the physical layer security techniques can be decomposed as follows [12]: i) information-theoretic security, ii) artificial-noise-based [13], iii) security-oriented beamforming techniques [14], iv) diversity-assisted security approaches [15], v) physical-layer secret key generation [16] and vi) spectrum sharing methods (See Fig.1). The secrecy capacity of wireless communications when there are eavesdroppers may be severely degraded due to the presence of a time-varying fading. In this regard, it is defined the ergodical secrecy-capacity to cope with the channel variations [17]. In [8] it was analyzed from an information-theoretic point of view the secrecy capacity when the legitimate transmitter and eavesdropper use multiple antennas and the legitimate user had Channel State Information (CSI) or partial CSI of the wiretap channel. Here we have referenced some papers on physical layer security schemes. This is a very short list on physical layer security schemes. However, for a more detailed references, the following surveys can be consulted [17]- [21]. This paper is divided in the following sections. First we introduce a section

on preliminaries of security levels. Next, in the third section we address the particularities of the satellite channel in terms from the security point of view. Section IV and V introduce some considerations that the physical layer security schemes have to take into account for providing certain level of security in the satellite beams and the multiple access scheme respectively. Section VI explains the signal model of the legitimate and eavesdopper considering time-packed waveforms. Finally, Section VII provides the secrecy-capacity of the proposed time-packed IoT system and in Section VIII we draw the main conclusions of this paper.

B. Motivation of the Work

The work presented in this conference departs from two previous works presented in this fora [22], [23]. In the first one, we showed how it was possible to increase the spectral efficiency of DVB-S2 signals by resorting to the frequency packing strategy. In the second one, we developed a system level simulator of Ultra Narrow Band (UNB) signals that directly access to the satellite. The conclusion of the first work was that in presence of residual interference such as the one that it is present in the four color satellite channel, frequency packing techniques were more suitable for waveforms with low-modulation formats. The conclusion of the second work was that the time duration of the UNB frames increases their collision probability as well as the Doppler-spread effect, which degrades its system level capacity. However, IoT devices generally work with low-modulation formats, such as DBPSK, or QPSK as much. So, the introduction of time packing techniques arose as a natural way to reduce the time duration of the UNB frames and reduce its Doppler effect. The relationship with security is due to the time packing strategy introduces a residual interference between the pulse-shapes that can be controlled by the transmitter. As a result, it makes the task of the potential eavesdroppers difficult. This approach is similar to the artificial noise one, but here the signal of information introduces the distortion instead of sending a secondary one, which it is quite inefficient in terms of energy. We consider that this solution can be of high utility in the satellite communications since the channel is mainly a Line Of Sight (LoS) one. Specifically, the overlapping between pulse shapes can be used to build a private key for each user of the physical layer. By doing so, the eavesdropper has to identify the overlapping degree that the legitimate user is using in its pulse-shapes. Nevertheless, the presence of a residual interference make the task of getting perfect estimations of the overlapping degree between the pulse shapes difficult. So, certain level of secrecy-capacity is obtained by using this strategy.

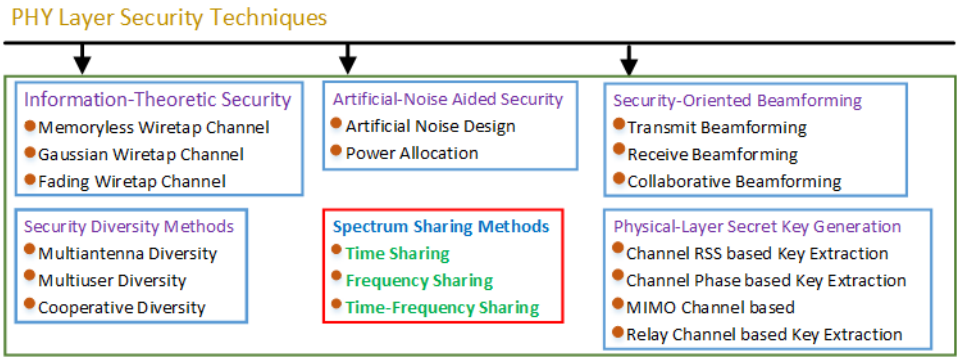


Figure 1: Taxonomy of the physical layer security techniques.

II. Preliminaries

In this section we introduce some concepts on the different types of secrecy levels and the main model used in physical layer security to study it that will be used along the paper.

A. Alice-Bob-Eve model

The general model of physical layer security problem is based on three main actors. The first one is the legitimate transmitter node, denoted as Alice. Next, the second actor is the legitimate receiver node, which it is referred as Bob. Finally, the third node represents the malicious node, the eavesdropper, and it is called Eve. According to this configuration, Alice wants to send to Bob packets of data in a secret way. The communication channel between Alice and Bob is denoted the main channel. However, the main goal of Eve is to intercept the messages from Alice to Bob, i.e. the legitimate entities, from its observations. To the communication channel between Alice and Eve is denoted the wiretap channel, i.e. the channel between the legitimate transmitter and the eavesdropper. This model was used by Wyner in [4] to lay the foundations of Physical Layer Security (PLS). Specifically, it showed that it was possible to setup a confidential communication between the legitimate user and receiver without sharing a secret key if the channel of the eavesdropper, i.e. wiretap channel was a degraded version of the one between the legitimate transmitter and receiver, i.e. main channel. This situation does not happen in practical scenarios since there is an inherent fading in the communication channels that can reduce the SINR of the legitimate transmission in favor of the eavesdropper one.

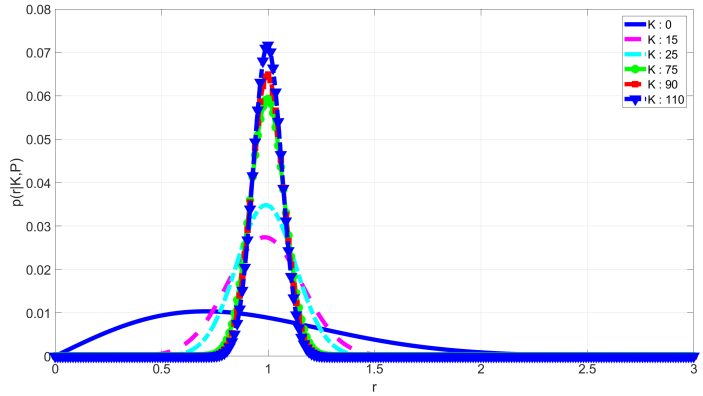


Figure 2: Rice distribution in terms of the K parameter.

B. Levels of Secrecy

Once it is developed an strategy at the physical layer for providing security, it is necessary to measure the level of security that it offers. The so-called secrecy. Specifically, there are the following types of security [17]:

- **Perfect Secrecy**: The mutual information leakage to Eve must be zero regardless of its processing power and computational capabilities. This is the most stringent secrecy measure as it ensures almost unit decoding error probability if the entropy of the message is the same as the key.

- **Ideal Secrecy**: The asymptotic conditional entropy of both the message and the key does not go to zero as the codeword length goes to infinity. This means that an encryption algorithm is ideally secure if no matter how much of cipher text is intercepted by Eve, there is no unique solution of the plaintext but many solutions of comparable probability.

- **Weak Secrecy**: The asymptotic mutual information rate goes to zero as the codeword length goes to infinity. Thus, this notion does not strictly force mutual information leakage to be zero on each channel use, but rather on average.

- **Strong Secrecy**: The asymptotic mutual information goes to zero as the codeword length goes to infinity. Thus, this notion forces mutual information leakage to be zero on each channel use, but not on average as in weak secrecy.

- **Semantic Secrecy**: It means that it is asymptotically impossible to estimate any function of the message better than to randomly guess it without knowing or considering Eve's observations and over all message distributions.

- **Distinguishing Secrecy**: It means that the channel output observations are asymptotically indistinguishable for different input information messages. This achieves strong secrecy over all message distributions.

As you can observe there are different levels of secrecy according to the message length that sends the legitimate transmitter -Alice-, the computational capacities and information level that the Eavesdropper -Eve- has about the communication channels. Consequently, it means that a service can be protected with different levels of security according to the price that the user can pay for it i.e. -Bob-. This is the so-called Physical Security As A Service (PSaaS) business model. Pay as the physical security that you need [17].

Next we introduce in the following section the particularities of the satellite channel from the point of view of security.

III. Satellite Channel Model

Regarding the statistical channel, we assume that the channel amplitude has some time variations. If this variation is small, then it can be modeled as a Rician distribution [24]- [26]. The Rician channel is the superposition of a constant signal and another one that varies in a random way as:

$$h_{Rician} = a + \sqrt{2 \cdot \sigma^2} \cdot h_{Random} \tag{1}$$

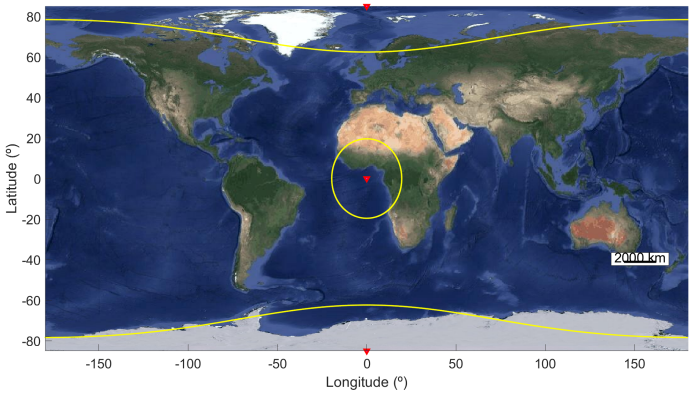


Figure 3: Coverage area of a LEO satellite at h=1400 Km altitude at the Poles and Equatorial Regions.

Being a the parameter that models the Line Of Sight (LoS) component whereas h_{Random} is a Complex Gaussian signal of zero mean and deviation σ. In this situation, if r denotes the channel's envelope, i.e. $r = |h_{Rician}|$, then the Rician probability distribution function is described as [26]:

$$f(r|K,P) = \frac{2 \cdot r \cdot (K+1)}{P} \cdot e^{\left(-K - \frac{(K+1) \cdot r^2}{P}\right)} \cdot I_0\left(2 \cdot r \cdot \sqrt{\frac{K \cdot (K+1)}{P}}\right), (r \geq 0) \tag{2}$$

where P is the channel power; equated as $P = a^2 + 2 \cdot \sigma^2$, whereas K is the so called vanishing factor of the Rician distribution and represents the relationship between the LoS power component and the random one and it is computed as:

$$K = \frac{a^2}{2\sigma^2} \tag{3}$$

Thus, from (3) if the vanishing factor $K \to \infty$, then the deviation of the random component of the channel goes to zero, i.e. $\sigma \to 0$, and so, the power of the LoS component tends to P. Conversely, if $K \to 0$, then the LoS component of the channel goes to zero, i.e. $a \to 0$, whereas the power of its random part goes to P, i.e. $2 \cdot \sigma^2 \to P$. Note from (2) that if we increase the K parameter the distribution of the signal tends to a Gaussian one which mean closes to the power of the LoS component and smaller variance. For a better understanding, Fig. 2 shows the form of the Rice distribution when $K \in \{0, 15, 25, 75, 90, 110\}$ and the channel power P is the unity, i.e. $P = 1$. Note in Fig. 2 that if we increase the K parameter the distribution of the signal tends to a Gaussian one which mean closes to the unity and smaller variance. In this situation the channels of the legitimate user and the eavesdropper are practically the same and so, the secrecy capacity is reduced. This case happens in satellite communications since the magnitude of the vanishing factor K is around $K \in \{17 - 20\}$ dB [27], [28]. At this point we have to remark that we have no assumed that the eavesdropper and legitimate user's channels could be located in different environments [29]. Otherwise, the geographic positions and the elevation angles of the legitimate user and the eavesdropper may impact on the secrecy-capacity. However, this part has been considered out of the scope of this work. Next, we provide in the following section some security considerations for the satellite beams.

IV. Considerations on the Satellite Beam from the Security Point of View

As it is known the beam of a satellite provides service in a region of Earth, the so-called footprint. This region can be quite extent and so it has some implications from the security point of view. So, whatever physical layer security system that wants to operate in the satellite domain has to be susceptible to them. Otherwise, it will fail to provide a larger secrecy level in the satellite domain. These considerations are the following:

1) *Earth is not a perfect sphere:* The flatness of Earth increases the coverage area of the satellites at larger latitudes. Fig. 3 shows the footprint of a LEO satellite at h=1400 Km altitude, i=98° degrees of inclination, user terminal elevation angle of θ = 5° when it crosses the poles and the equatorial regions. Note the large difference between the footprints of these two scenarios. In terms of security, it means that the potential eavesdroppers could overhear the information of the legitimate user at further distances from it when it is positioned at larger latitudes (e.g. poles) than at lower ones (e.g equatorial region).

2) *Presence of Co-channel interference:* Generally the satellite beams are designed to consider a co-channel interference at their centers 3 dB lower than at their borders [24]. From the security point of view it means that it is key the relative position of the eavesdropper respect to the legitimate user but also their position inside the beam. Note that the satellite beams may be fixed (e.g. GEO satellites). However, the IoT devices could have certain degree of mobility or be static and

located in cities/industries/infrastructures placed at the border of the satellite beams. In these situations, the eavesdropper may have a similar/better co-channel interference than the legitimate user has.

3) *Line of Sight (LoS) Satellite Channel:* Note that the satellite channel model has a large Line of Sight (LoS) component. So, it means that the channel of the eavesdropper and the legitimate user could be quite similar in the same beam. This fact reinforces the idea of using time-packing since it introduces an artificial multi-path interference that degrades the eavesdropper's channel (See Fig.5b)).

4) *Geographic dependence of the Security:* The flatness of the poles and the presence of a co-channel interference make us to consider that the secrecy-capacity depends on geographic information. However, time-packing strategies permit to modify the overlapping degree in order to increase the secrecy-capacity with independence of the coordinates in which the IoT devices be positioned. In particular it means that at higher latitudes the information of the satellite beams would have to be encoded with a larger overlapping degree, i.e. τ, to guarantee the same security level than the lower latitudes have.

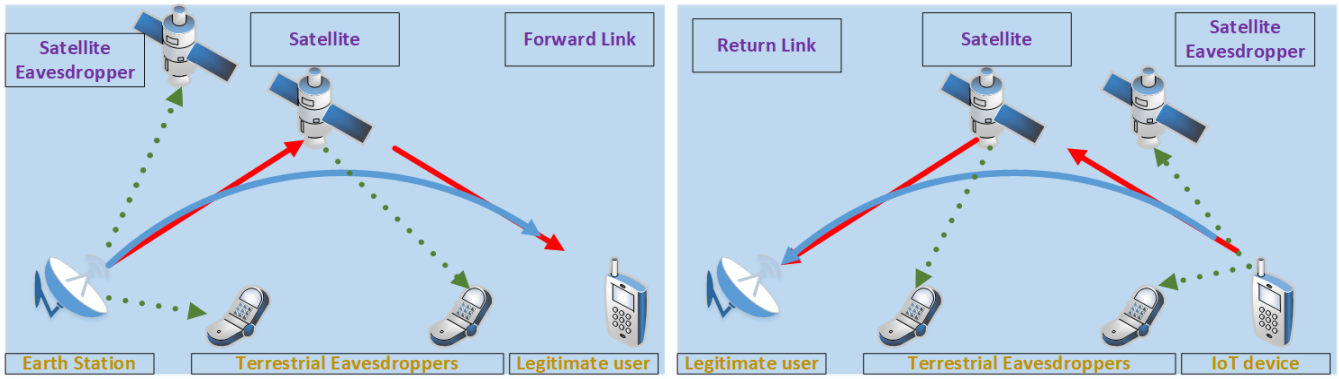
V. Consideration of the IoT Multiple Access Channel from the Security Point of View

IoT systems generally resorts to a variant of the classical Aloha protocol to communicate multiple IoT devices with the gateway. For instance, Sigfox and NB-IoT systems use random Aloha protocol with time repetitions. Towards this regard, the success probability in the time-frequency slotted Aloha when the packets are uniformly distributed in the frequency and time domains is [30]:

$$P_{Success} = e^{-2\times 2\times G_{T,F}} \tag{4}$$

being $G_{T,F}$ the traffic load of the un-slotted Time-Frequency Aloha protocol, which it is defined as $G_{T,F} = N \times T_S \times n_r/(T \times B)$, being N the packet length, T_S the symbol time, n_r the number of replies, T is the average transmission period and B symbolizes the bandwidth of the available channel. Towards this regard, the increase in the number of repetitions improve the success probability of the access scheme and the detection of the data. This is valid not only for the legitimate receiver -Bob- but also for the eavesdropper -Eve-. For that reason, it would be interesting to reduce the temporal duration of the frames, which augments the success probability of the access, but without augmenting the signal bandwidth. By doing so, it is made the overhearing task of the eavesdropper more difficult. This strategy fits with the signal model of using time packing, since it shrinks the temporal duration of the frames without increasing the signal bandwidth. The price to pay is that appears an interference, which introduces complexity on the detector, but from the secrecy point of view augments the secrecy rate. At this point we would like to remark that the increase of the duration of the transmission frames, i.e. including replies, could introduce a Doppler spread in case that the IoT receiver was mobile.

Finally, we present the signal model of the legitimate user and eavesdropper when the transmitted waveform is encoded using a time-packed strategy.



(a) Satellite Forward Link with the legitimate user and potential eavesdroppers.(b) Satellite Return Link with the legitimate user and potential eavesdroppers.

Figure 4: Satellite Links with the legitimate user and potential eavesdroppers

VI. Signal Models

In this section we present the signal models of the legitimate user and eavesdropper for a satellite link.

A. Signal Model of the Legitimate and Eavesdropper

In the following we provide the mathematical expressions that describe the signal model of the legitimate user and the eavesdropper. In the satellite field, we have the forward and the return links. In the forward link, the transmitted signal departs from the Earth-Station and it is received by the IoT device, i.e. the legitimate user. On the return link, the IoT device sends the information to the Earth-Station, which would take the role of legitimate receiver. In both cases the eavesdropper could be located either at the space or on the terrestrial surface (See Figs. 4a-4b). In any case, the transmitted time-packed message at the k-th time instant is given by [6], [7]

$$x_d[k] = \sum_n s_d[n] p_l[k - nM_{TP}], \tag{5}$$

where $s_d[n]$ and $p_d[k]$ are the *n*-th information symbol of the packet and the pulse that shapes the desired signal transmitted, and M_{TP} is the separation between consecutive pulses according to the time-packing strategy. If M denotes the oversampling factor and τ the overlapping degree between pulses, then their relationship will be:

$$\tau = 1 - \frac{M_{TP}}{M}, \qquad (0 < M_{TP} \leq M) \tag{6}$$

If the separation between two consecutive time-packed pulses (in oversampled samples), M_{TP}, was equal to the oversampling factor, M, i.e. $M_{TP} = M$, then the overlapping degree would be zero, $\tau = 0$, and we would have the Nyquist sampling case. Next, under flat fading conditions, the signal received by the legitimate user is

$$d_l[k] = h_l[k] \cdot x_d[k] + \sum_{q=1}^{N_I - 1} h_{l,q}[k] \cdot x_q[k] + \eta_l[k], \tag{7}$$

where $h_l[k]$ is the channel impulse response from the transmitter to the legitimate user, x_d is the desired information, N_I is the number of time-packed interference symbols, and $\eta_l[k]$ represents the additive noise plus the residual co-channel interference term from other beams, which it is formulated as

$$\eta_l[k] = \sqrt{I_l} \sum_{p=0}^{K_I - 1} h_{l,p}[k] \cdot x_p[k] + \sqrt{P_{n_l}} \cdot \upsilon_l[k], \tag{8}$$

being I_l and P_{n_l} the power of the co-channel interference and the Additive White Gaussian (AWG) noise that degrade the channel of the legitimate user. Similarly, the signal model that receives the eavesdropper will be:

$$d_e[k] = h_e[k] \cdot x_d[k] + \sum_{q=1}^{N_I - 1} h_{e,q}[k] \cdot x_q[k] + \eta_e[k], \tag{9}$$

where $h_e[k]$ is the channel impulse response from the transmitter to the eavesdropper -so called the wiretap channel- and $\eta_e[k]$ represents the additive noise plus the residual co-channel interference term from other beams, which it is formulated as

$$\eta_e[k] = \sqrt{I_e} \sum_{p=0}^{K_I - 1} h_{e,p}[k] \cdot x_p[k] + \sqrt{P_{n_e}} \cdot \upsilon_e[k], \tag{10}$$

At this point, Fig.5a- 5b show five consecutive square root raise cosine pulse-shape waveforms with roll-off factor of $\rho = 0.1$, bandwidth of BW=8KHz and oversampling factor of 10 when their overlapping degree is $\tau = \{0, 25\}\%$. The case of τ = 0 $\%$ represents the situation of classical Nyquist-pulses, i.e. there is no Inter-Symbol Interference (ISI) between the consecutive pulses (See Fig.5a). On the contrary, if the overlapping degree τ augments (e.g. $\tau = 25\%$), then the ISI increases (See Fig.5b). Generally, the presence of ISI in a communication channel has been considered as an impairment. Nevertheless, this type of ISI can be controlled by the transmitter. So, it means that the parameter τ may be used to build a secret key of the physical layer.

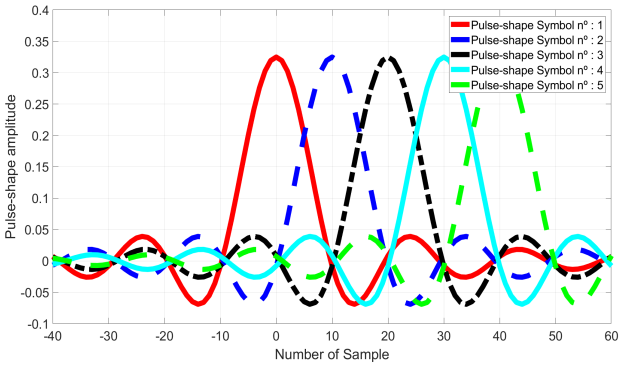
After presenting the signal models of the legitimate user and the eavesdropper, we introduce the secrecy-rate for a time-varying channel. The following section details it.

VII. Secrecy-Capacity

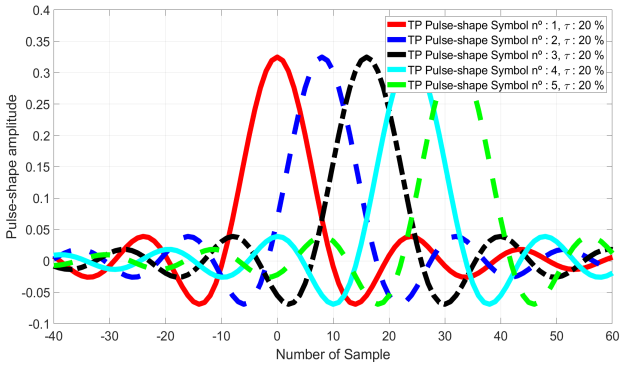
Generally speaking, secrecy-capacity is determined by the main channel, i.e., the channel between the transmitter and the legitimate user, and the wiretap channel, i.e. the channel between the transmitter and the eavesdropper. The secrecy-capacity for an instantaneous value of the channel in the quasi-static fading scenario is [21], [31]:

$$C_S = I_l(\mathbf{s}[n]; y_l[n]) - I_e(\mathbf{s}[n]; y_e[n]), \tag{11}$$

being $I_l(\mathbf{s}[n]; y_l[n])$ and $I_e(\mathbf{s}[n]; y_e[n])$ the mutual information of the legitimate user and the eavesdropper respectively. However, the instantaneous secrecy-capacity is different for each channel fading realizations. In order to evaluate the security in a long-term sense, i.e. across multiple coherent time slots, average secrecy-capacity was proposed in [32] as performance metric. To



(a) Nyquist pulse-shape, τ=0% of overlapping. Pulses with No-ISI.



(b) Time-packed pulse-shape, τ=20% of overlapping. Pulses with ISI.

Figure 5: Pulse-shapes without and with ISI.

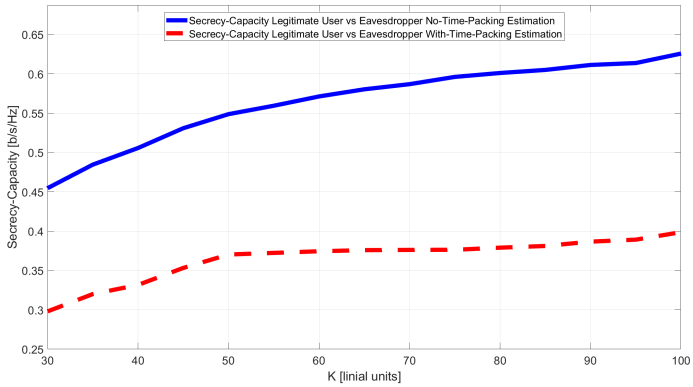


Figure 6: Secrecy-Capacity of the legitimate user respect the two possible types of eavesdroppers when the overlapping degree is $\tau = 25\%$(See Section II)

be more specific, the average secrecy-capacity is equal to the maximum average instantaneous secrecy-capacity over fading channels and formulated as:

$$\underset{max}{C_S} = \int C_S(h_l, h_e) \cdot p(h_l) \cdot p(h_e) \cdot dh_l \cdot dh_e, \tag{12}$$

In order to model the eavesdropper, we can assume that it has or not ant knowledge of the waveform that it is using the legitimate transmitter -Alice-. If it does not have any knowledge, then we can assume that it is or not able to estimate the distance between the pulse-shapes. If not, the transmitter is always able to transmit with perfect secrecy the data. On the contrary, there is a region in which it can transmit with secrecy (weak secrecy). The reason is that there is a multipath interference due to the time-packing effect that it unknows. On the contrary, if the eavesdropper knows that the legitimate user is transmitting with a time-packed waveform, then it is still possible to transmit with a certain level of secrecy. In this situation, the eavesdropper has to estimate the overlapping degree between pulse-shapes. Here the residual interference between beams impedes to obtain perfect estimates of the overlapping degree between pulses which permits to asses still a certain level of secrecy (weak secrecy). Next, Fig.6 shows the secrecy-capacity when the vanishing factor of the channel varies from K=30 to K=100 in steps of 5. The overlapping degree between the consecutive pulses is $\tau = 20\%$. There the residual co-channel interference and the noise power of the legitimate user and the eavesdropper are equal to $I_l = I_e = -15$ dB and $P_{n_l} = P_{n_e} = -10$ dB respectively. The results show that if it used time-packing to encode the transmission data, then exists a secrecy-capacity region at large vanishing factors of the Rician channel. As a result, it means that the transmitter can select a rate, so-called secrecy-rate that falls in the outage region of the eavesdropper's capacity. In this situation the eavesdropper is not able to decode the *plaintext* message and so, it is guaranteed the secrecy of the communications.

VIII. Conclusion

In this paper we have evaluated the technique of time-packing as alternative to the well-known artificial noise technique for increasing the secrecy-capacity of IoT communications over satellite. Note that the satellite channel model has a large Line of Sight (LoS) component. So, it means that the channel of the eavesdropper and the legitimate user could be quite similar in

the same beam. However, the use of the time-packing technique introduces an artificial multi-path interference that degrades the eavesdropper's channel. In this case, we have considered two types of eavesdropper: i) without being able to estimate the time-packing multi-path, and ii) equipped with an estimation block of the time-packing interference. In the first case, all interference signals are considered as noise whereas in the second one part of the interference is assumed as noise. In both cases, it is possible to obtain a secrecy-capacity. Finally, comment that in the satellite field there is a residual co-channel interference. This interference limits the resolution of the eavesdroppers although they be equipped with multiple antennas. Consequently, in this paper we have considered that eavesdropper does not have full knowledge of the time-packed multi-path interference. Similar approach was followed in [33]. However, there the rain losses made difficult to obtain perfect channel estimations.

ACKNOWLEDGMENTS

This work has received funding from the Spanish Ministry of Science, Innovation y Universities under project TERESA-TEC2017-90093-C3-1-R (AEI/FEDER,UE); and from the Catalan Government (2017 SGR 891 and 2017 SGR 1479).

REFERENCES

[1] European Telecommunications Network Operators' Association (ETNO), "Annual Economic Report 2018", December 2018.
[2] International Data Corporation,"Worldwide Semiannual Internet of Things Guide", December 2018.
[3] D. Minoli, K. Sohraby, J. Kouns,"IoT (IoTSec) Considerations, Requirements, and Architectures", In Proc. Of IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1006–1007, January 2017.
[4] A.D. Wyner,"The wire-tap channel",Bell. Sys. Tech. J., vol.54,pp.1355- 1387,1975.
[5] H. Rahbari, M. Krunz, "Secrecy beyond Encription: Obfuscating Transmission Signatures in Wireless Communications," In Proc. IEEE Communications Magazinne, vol. 53, pp. 54–60, December 2015.
[6] A. Modenini, "Advanced transceivers for spectrally efficient communications", Ph.D. dissertation, Jan. 2014.
[7] F. Russek and A. Pralja,"Optimal Channel Shortening for MIMO and ISI Channels", In Proceedings of IEEE Trans. On Wireless Communications, vol.11,n2,pp. 810-818, February 2012.
[8] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constrains", In Proc. of IEEE, vol. 103,n.10, pp.1747–1761, October 2015.
[9] G. Zheng, P. Arapglou, B. Ottersten,"Physical Layer Security in Multibeam Satellite Systems", In Proc. Of IEEE Transactions on Wireless Communications, vol.11,n.2,pp. 852–862, February 2012.
[10] Y.Xiao, et al,"MAC security and security overhead analysis in the IEEE 801.15.4 wireless sensor networks," EURASIP J. Wireless Comm. Networks, 2006.
[11] M. Frustaci, et al, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", In Proc. Of IEEE Internet Of Things Journal, vol. 5,n.4, pp. 2483-2495, August 2018.
[12] Y. Zou, et al,"A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", In Proc. Of The IEEE, vol. 104,n.9, pp.1727-1765, September 2016.
[13] O.Cepheli, T. Maslak, and G. Kurt, "Analysis on the effect of artificial noise on physical layer security,"In Proc. Signal Processing Comm. Appl. Conf. Haspolat, Turkey, pp.1-4, Apr. 2013.
[14] J.Wu,and J.Chen, "Multiuser transmit security beamforming in wirless multiple access channels," In Proc. IEEE Int. Conf. Commun., Ottawa, Canada, pp.903-906, Jun.2012.
[15] Y.Zou,X. Wang, and W.Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Comm., vol.6, nº.12,pp.5103-5113,Dec.2013.
[16] Q.Wang,, et al, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," In Proc. IEEE Int. Conf. Comput. Commun., Shangai, China, Mar. 2011.
[17] J.M.Hamamreh,H.M. Furqam, and H.Arslan,"Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey", In Proc. of IEEE Comm. Surveys & Tutorials, vol.21,n.2, second quarter,pp.1733-1828, 2019.
[18] Y. Liu, H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges", In Proc. IEEE Communications Surveys & Tutorials, vol.19, n.1,pp.347 - 376, August 2017.
[19] Y. Wu, et al,"A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", In Proc. Of IEEE Journal On Selected Areas in Communications, vol.36,n.4,pp.679-695, April 2018.
[20] V. Hassija et al, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", In Proc. Of IEEE Access, vol.7,pp. 82721 - 82743, June 2019.
[21] Y. Gao, H. Ao, Z. Feng, W. Zhou, S. Hu, X. Li,"Modeling and Practise of Satellite Communication Systems using Physical Layer Security: A Survey", In Proc. Of IEEE International Conference on Computational Science and Engineering (CSE), pp.829-832, July 2017.
[22] J.Bas et al,"Mutual Information Analysis of Frequency Packing Schemes in Multi-Beam Satellite Systems", In Proc. Of Ka band Conference,Trieste, Italy, October, 2017.
[23] J.Bas et al,"Practical Considerations For System-Level Simulators of UNB IoT Devices Over LEO Satellites", In Proc. Of Ka band Conference,Niagara Falls, Canada, October, 2018.
[24] Maral, "Satellite Communication Systems: Systems, Techniques and Technology", in Wiley, 5th Edition, 2011.
[25] F. Pérez-Fontán et al, "Statistical Modeling of the LMS Channel," In IEEE Trans. On Vehicular Technology, vol.50,nº6,Nov. 2001,pp.1549-1567.
[26] F.Pérez-Fontán, P.Mariño,"Modeling the Wireless Propagation Channel", Published by Wireless Series on Communications,2008.
[27] ETSI TR 102 376 v.1.1.1 (2005-02), "Digital Video Broadcasting (DVB); User guidelines for the second generation system for Broadcasting, Interactive Service, News Gathering and other broadband satellite applications (DVB-S2)".
[28] ETSI TR 102 768 v1.1.1 (2009-04), "Digital Video Broadcasting (DVB); Interaction channel for Satellite Distribution Systems; Guidelines for the use of EN 301 790 in mobile scenarios".
[29] ITU-R P.618-13, "Propagation data and prediction methods required for the design of Earth-space telecommunication systems", December 2017.
[30] A. Tannenbaum, "Computation Network", Pub. by Princeton 1992.
[31] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao,"A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", In Proc. Of IEEE Journal on Selected Areas in Communications, vol.36, n.4, pp.679-695, April 2018.
[32] P.K.Gopala,L.Lai, and H.E. Gamal,"On the secrecy capacity of fading channels,",IEEE Transcations Inf. Theory,vol.54,no10,pp.4687-4698,Oct. 2008.
[33] G. Zheng, P. Arapoglou, B. Ottersten,"Physical Layer Security in Multibeam Satellite Systems", In Proc. Of IEEE Transactions on Wireless Communications, vol.11,n.2,pp. 852–862, February 2012.